REMARKS

In the Office Action dated June 16, 2006, claims 13-23 were rejected. Claims 13-23 are now pending in the application. In view of the remarks and amendments, Applicant respectfully requests reconsideration of the application.

Examiner objects to Claims to 19-23 if Claims 13, 14, and 16-18 were found allowable. Applicant has amended Claim 19 to overcome this objection.

Claims 13, 16, 19 and 21 were rejected under U.S.C. § 103(a) as being unpatentable over the Koopman reference (US Patent 5,696,828) in view of the Wilson reference (US Patent 5,295,188).

However, in marked contrast to the Koopman reference and the Wilson reference both singly and in combination, amended Claims 13 and 19 include the limitation, in part, of:

> performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large random pads wherein the plurality of large random pads have less entropy than the plurality of shuffled large random secrets;

and

> performing an exclusive OR function on the plurality of randomly rotated and randomly shuffled large random pads to produce a final pad wherein the final pad has less entropy than the plurality of randomly rotated and randomly shuffled large random pads;

The Examiner recites sections column 5, line 60-column 6, line 22 and column 7, lines 22-33 from the Koopman reference for the portions of Claims 13 and 19.

For example, the Koopman reference states that to insure randomness of the numbers generated by the system, an additional algorithmic step is performed. A portion of each compressed sample are input into an exclusive OR simultaneously with an independently varying, guaranteed non-repeating value such as the date and time of day. (Koopman, column 7, lines 22-33) In this case, the exclusive OR function is utilized such that "some variation is instituted in the input of the one way encryption algorithm in the event an unintentionally repetitive data input exists. By applying the exclusive OR function to an limitless random value and a non repeating value, the Koopman reference teaches the use of the resultant output from the exclusive OR function to have the same entropy as the limitless random value input for the exclusive OR function since the non repeating value has no or very little intrinsic entropy, i.e. it is a non random value.

In marked contrast to the Koopman reference, the invention as described in Claims 13 and 19 claims that a plurality of large random pads (the resultant output from the exclusive OR function) has a reduced entropy compared to the plurality of shuffled large random secrets (the input to the exclusive OR function).

In fact, the Koopman reference teaches away from the invention as recited in Claims 13 and 19 by teaching that the use of "an independently varying, guaranteed non-repeating value such as the date and time of day" as an input to the exclusive OR function. (Koopman, column 7, lines 22-33)

Further, the Wilson reference fails to teach performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large

random pads wherein the plurality of large random pads have less entropy than the plurality of shuffled large random secrets, as recited in Claims 13 and 19.

In addition, Claims 13 and 19 further recite that the plurality of mixing keys, the plurality of random rotation values, and the plurality of working keys are random and secret. In marked contrast, the Koopman reference teaches the use of a fixed relative prime number to provide the shuffling capability (Koopman, column 5, line 60 to column 6, line 22).

In marked contrast, the Wilson reference teaches the use of a non-random 4-let that is constructed from bit pairs, which ultimately come from the non-random plaintext that is to be encrypted (Wilson, column 6, lines 14-37).

Accordingly, Applicant respectfully submits that the Koopman reference and the Wilson reference either singly or in combination fail to hint, teach, or suggest the elements within independent Claims 13 and 19. Thus, independent Claims 13 and 19 are patentable over the Koopman reference in view of the Wilson reference and are now in condition for allowance. In addition, Claims 16 and 21 depend directly or indirectly on Claims 13 and 19, respectively and, therefore, are patentable for at least the same reasons discussed above.

Claims 14, 15, and 20 were rejected under U.S.C. § 103(a) as being unpatentable over the Koopman reference (US Patent 5,696,828) and the Wilson reference (US Patent 5,295,188) in view of the Ritter reference (US Patent 5,623,549).

Independent Claims 13 and 19 are patentable for the same reasons as discussed above. Claims 14 and 15 depend directly or indirectly on allowable independent Claim 13 and, therefore, are patentable for at least the same reasons discussed above. Claim 20 depends directly or indirectly on allowable independent Claim 19 and, therefore, is patentable for at least the same reasons discussed above.

Claims 17, 18, 22, and 23 were rejected under U.S.C. § 103(a) as being unpatentable over the Koopman reference (US Patent 5,696,828) and the Wilson reference (US Patent 5,295,188) in view of the Schneier reference (Applied Cryptography).

Independent Claims 13 and 19 are patentable for the same reasons as discussed above. Claims 17 and 18 depend directly or indirectly on allowable independent Claim 13 and, therefore, are patentable for at least the same reasons discussed above. Claims 22 and 23 depend directly or indirectly on allowable independent Claim 19 and, therefore, are patentable for at least the same reasons discussed above.

In view of the foregoing remarks and amendments, Applicants respectfully submit that all pending claims are in condition for allowance. Such allowance is respectfully requested.

If the Examiner finds any remaining impediment to the prompt allowance of these claims that could be clarified with a telephone conference, the Examiner is respectfully requested to contact Richard H. Butler at (408) 425-3376.

Respectfully submitted,

Dated: 9/15/06

Richard H. Butler
Registration No. 40,932

Please Send Correspondence to:
Valley Oak Law
5655 Silver Creek Valley Road
#106
San Jose, CA 95138
(408)425-3376